Acronis

acronis.com

Acronis Cyber Cloud

Integration with N-able N-central

Integration Guide

REVISION: 10/12/2023

Table of contents

Introduction

Integration overview

This document describes how to enable and configure the integration of Acronis Cyber Cloud with N-able N-central.

Once set up, the integration enables you to:

- Deploy Acronis on Windows devices
- Map Acronis customer tenants to N-able N-central customers
- Monitor protected devices
- Apply and revoke protection plans
- Run the following types of automated tasks - backup, antivirus scan, malware scan, vulnerability assessment and patch management
- Provision RMM customers to Acronis and configure automatic provisioning and deprovisioning of customers, triggered by changes in RMM

All this functionality is available from within N-able N-central, without having to go to the Acronis Cyber Protect web interface.

Glossary

- **MSP** - a Managed Service Provider, who uses both N-able N-central and Acronis Cyber Protect
- **Customer** - a client of the MSP
- **Partner tenant** - the account for an MSP on AcronisCyber Cloud
- **Customer tenant** - the account for a Customer on AcronisCyber Cloud

Permissions and roles

Only partner tenant users with Company Administrator roles are allowed to enable/disable or edit the integration.

All other users have Read-only access. This means that they can view, but not modify the integration settings.

Prerequisites

To use this integration, you should have:

- At least a single, fully configured N-able N-central account
- An AcronisCyber Cloud account with:
  - at least one Customer tenant set up
  - an active user with Acronis administration permissions
  - at least one protection plan configured to be used as the default one

Only customer tenants that are not in Self-service mode or don't have Support Access disabled, can be managed by the integration.

How the integration works

In N-central, the MSPs most often use custom properties together with Automation Manager policies that pull in the appropriate customer or device-specific information, rather than creating separate Automation Manager policies per customer or per device.

In this particular integration, you should define two custom properties:

- "Acronis Registration Token" - this property's value will be automatically populated over API from the Acronis Cloud. The value will be generated once customer mapping is applied/created.
  This advanced feature will be supported only for Windows OS as .amp files (automation policies) work on Windows only.

- "Acronis Data Center URL" - this is the Acronis URL for your tenant. Its value will be automatically set and maintained by the integration.

  Once the Acronis N-central customer mapping is applied, every 10 minutes the integration will create a new registration token for each mapped customer. If a default plan is selected, the token for this plan will include 'Apply protection plan'. If no default plan is selected, then the token will be just a registration one. Once the token is created, its value will be stored in Custom Property via an API call for that customer in N-central, so that the integration scripts can automatically use this token when executed.

Setting up the integration

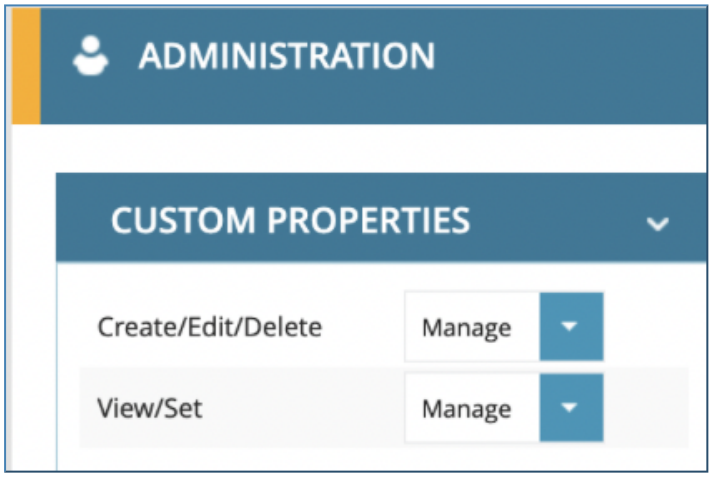
Setting up API user in N-able N-central

See below how to register API users in the N-able N-central portal.

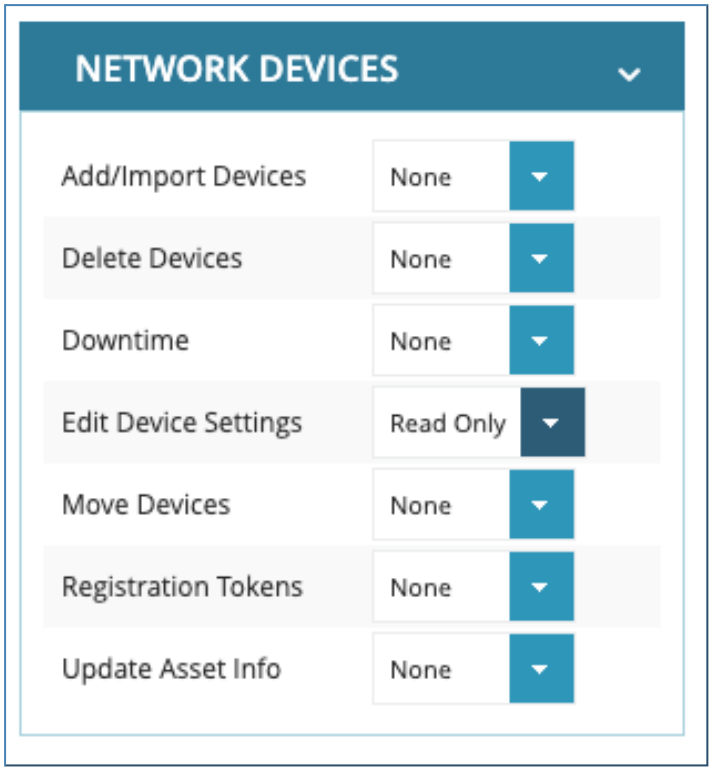
Configure API role

Note
It is possible to configure an already existing role, but you are still recommended to create a new, special API role with limited access.

1. Go to **Administration** > **User management** > **Roles** > **Create role**.
   See more details.
2. Provide a role name, for example **Acronis API role**.
3. Set this role the following permissions:
   - ADMINISTRATION > CUSTOM PROPERTIES > Create/Edit/Delete = 'Manage'
   - ADMINISTRATION > CUSTOM PROPERTIES > View/Set = 'Manage'



- DEVICES > NETWORK DEVICES > Edit Device Settings = 'Read Only'



4. Click **Save**.

Configure API user

Note
Although you can configure an existing user, you are highly recommended to create a special API user with limited access.

1. Go to **Administration** > **User management** > **Users** > **Create user**.
   See more details.
2. Define user parameters (for example, **Acronis API user**).
3. On the **Roles** tab, assign the **Acronis API role** created before.
4. On the **Access Groups** tab, assign a group with customers that have to be available for the integration.

   Note
   If not configured, customers will not be accessible for mapping in the Acronis console.

5. On the **API access** tab, preferably enable the **API-Only User** to limit access.
6. Make sure that 2FA is switched off for this user. If not, disable it from **User details** tab > **User information** > **Use Two-Factor Authentication**.
7. Save the user.

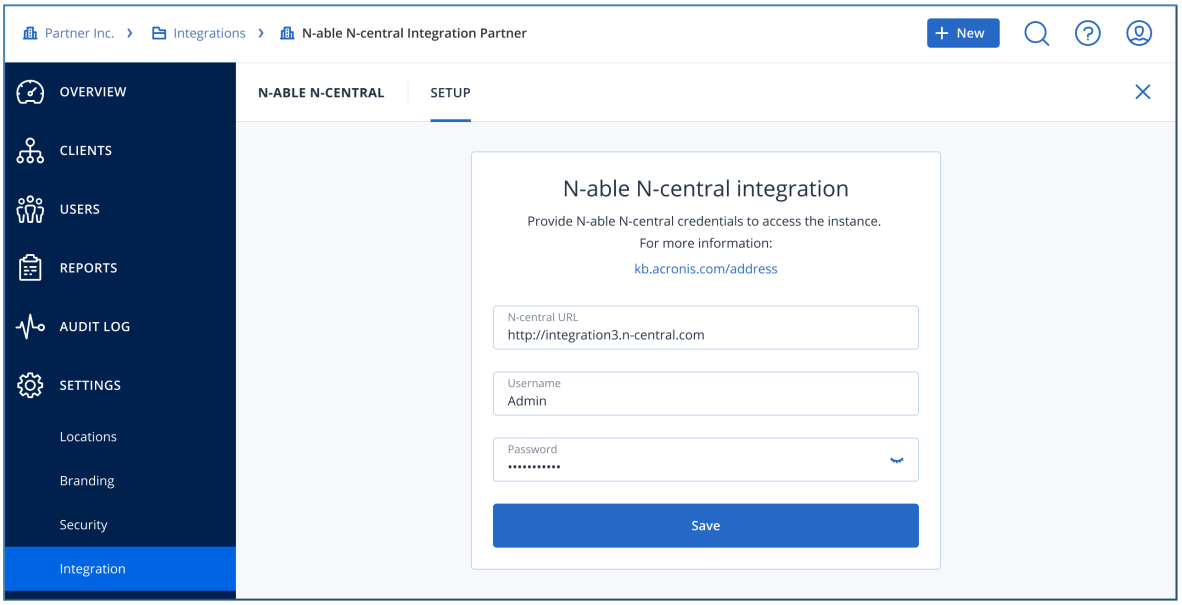
You can now proceed with enabling the integration.

Setting up integration in Acronis Management portal

See below how to enable and configure the integration in the Acronis Management portal before proceeding to configuration in N-able N-central.

Enable integration

1. Go to **Acronis Management portal** > **Integrations**.
2. Click on the **N-able N-central** tile.
3. Enter your integration credentials:
   - **N-central URL**
   - **Username**
   - **Password**



4. Click **Save**.
5. If connection is established successfully, you will be redirected to **Integration settings**.

Support for on-premise installations

The Acronis integration for N-able N-central does support on-premise installations. In such cases, verify that the following requirements are met before enabling the integration and entering the N-able credentials:

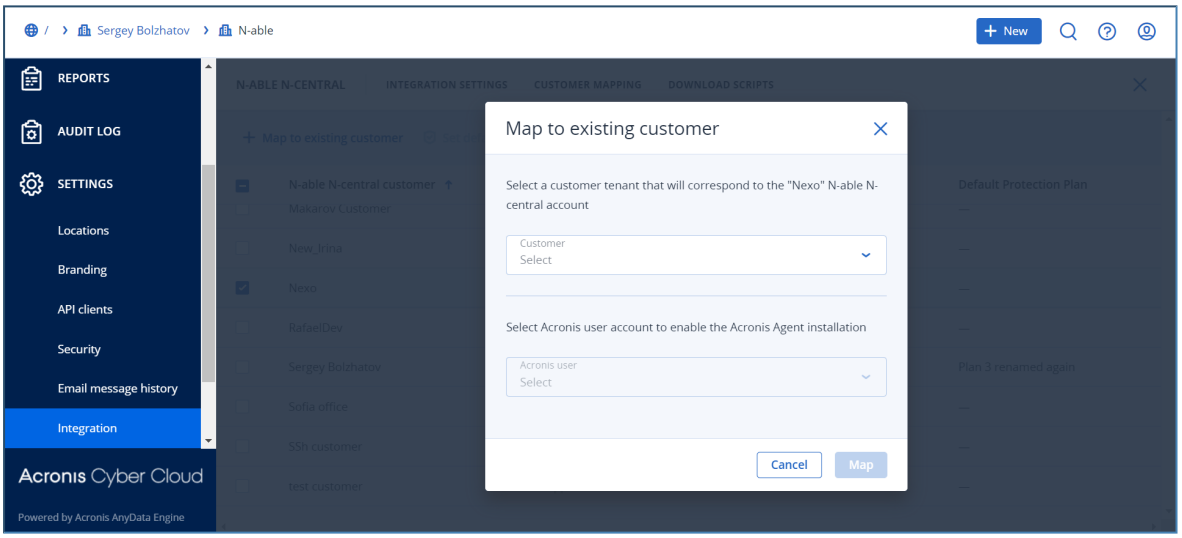
- The SSL certificate on your Web server is correctly installed, valid, trusted and doesn't produce any errors. For example, use any of the following checkers:
  - https://whatsmychaincert.com/
  - https://www.sslshopper.com/ssl-checker.html

- The default port used by the integration is TCP 443, so make sure that it is open in your firewall. The same applies if your on-premise installation is configured to use a different port.
- HTTP schema is ***not*** supported. Your installation can use HTTPS only.

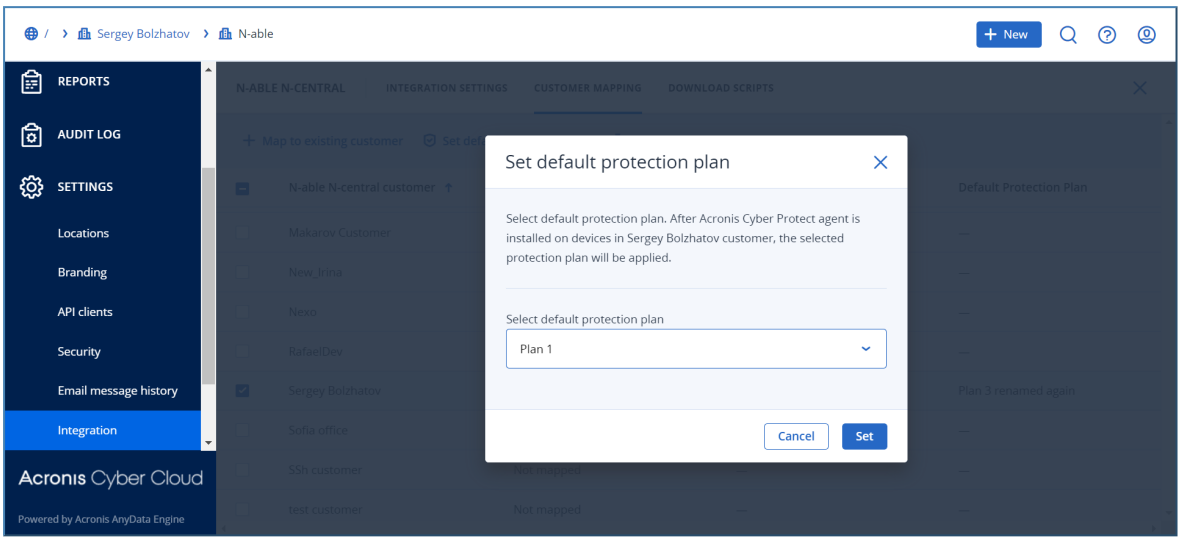
Apply company mapping

N-able N-central customers have to be mapped in order for the integration to be able to provision **Acronis Registration token** and **Data center URL** into customer's custom properties. These properties will be later required for the scripts to be run correctly.

1. Go to **Acronis** > **Customer Mapping** tab.
2. Use the list to select a customer that is not currently mapped.
3. Click the **Map to existing customer tenant** button in the action bar to display a popup with available customer tenants and some user fields.
4. Select an unmapped customer tenant and a user account, then click **Map**.
   The user selected for setting default protection plan should have Acronis administration permissions.



5. Click **Set default protection plan** in the action bar to display a popup with available protection plans.



6. Select a default protection plan, then click **Set**.

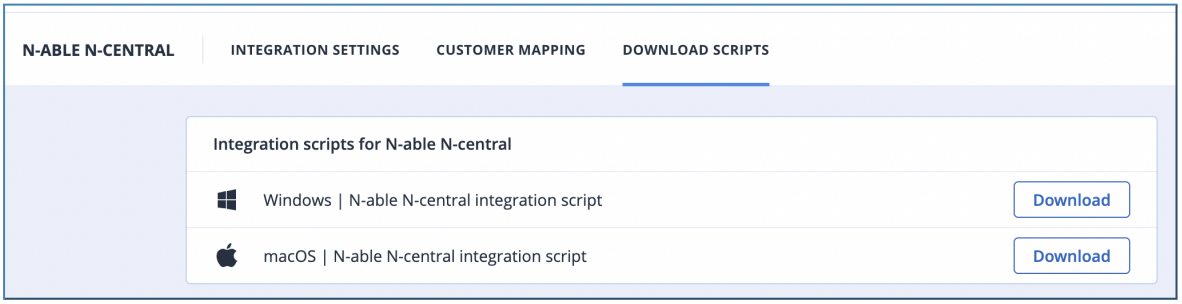
Note

Once you have mapped an Acronis Customer tenant to N-able N-central, you have the possibility to re-map it to another customer. To achieve that use the following workflow:

- Run uninstall script (See the Uninstall chapters)
- Re-map customer in Acronis Cloud UI
- Run install script (See the Deploy chapters)

Download scripts

1. Go to the **Download scripts** tab.
2. Download the available integration scripts packages:



These packages are required in order to proceed with the N-able N-central setup.

Setting up integration in N-able N-central

To set up the integration, you have to upload the scripts, downloaded from the Acronis Management portal and configure special Acronis custom properties.

Define custom properties

Configure custom properties required to run scripts:

1. Log into your N-able N-central instance.
2. Click **Administration** > **Custom Properties**.
3. Click **Add** > **By Customers** > **Text Type**.
4. Provide the following name: **Acronis Registration Token**.
5. Leave empty the default text value of the property.
6. Select the **Customers** and **Sites** that the new property will apply to.
7. Click **Save**.
8. Repeat the same procedure to create **Custom Properties** according to the table below:

	TYPE	PROPERTY NAME	DEFAULT TEXT	DESCRIPTION
1	By Customers\ Text Type	Acronis Registration Token	(empty)	Will be used to automatically store Registration token generated for every mapped customer. The value of the property is required to run scripts, e.g. to deploy the Acronis agent.
2	By Customers\ URL type	Acronis Data Center URL	(empty)	Will be used to automatically store Acronis Data Center URL for every mapped customer. The value of the property is required to run scripts, e.g. to deploy the Acronis agent.
3	By Customers\ Text Type	backup	**backup**	An input parameter for the "Acronis_ scans" script to run backup
4	By Customers\ Text Type	av_scan	**av_scan**	An input parameter for the "Acronis_ scans" script to run Antivirus scan
5	By Customers\ Text Type	malware_scan	**malware_scan**	An input parameter for the "Acronis_ scans" script to run malware scan
6	By Customers\	vulnerability_ assessment	**vulnerability_ assessment**	An input parameter for the "Acronis_ scans" script to run vulnerability

	TYPE	PROPERTY NAME	DEFAULT TEXT	DESCRIPTION
	Text Type			assessment
7	By Customers\ Text Type	patch_ management	**patch_ management**	An input parameter for the "Acronis_ scans" script to run patch management

Configure device monitoring custom properties that will be automatically populated with values for all devices under mapped customers:

1. Log into your N-able N-central instance.
2. Go to **Administration** > **Custom Properties**.
3. Click **Add** > **By Devices** > **Text Type**.
4. Provide the following name: **Acronis Agent version**.
5. Leave empty the default text value of the property.
6. Select the **Operating systems** and **Device Classes** the new property will apply to.
7. Click **Save**.
8. Repeat the same procedure to create custom properties, according to the table below:

	TYPE	PROPERTY NAME	DEFAULT TEXT	DESCRIPTION
1	By Devices\ Text Type	Acronis Agent version	(empty)	Current version of the Acronis agent, installed on the device
2	By Devices\ Text Type	Acronis Alerts	(empty)	Number of active alerts for the device (0 if none)
3	By Devices\ Text Type	Acronis CyberFit score	(empty)	Security assessment scoring rate that evaluates the security posture of the device. See https://www.acronis.com/en-us/support/documentation/CyberProtectionService/#cyberfit-score-for-machines.html?Highlight=CyberFit%20Score
4	By Devices\ Text Type	Acronis Days since last backup	(empty)	Number of days since last successful backup run for the device
5	By Devices\ Text Type	Acronis days since last malware	(empty)	Number of days since last successful malware scan run for the device

	TYPE	PROPERTY NAME	DEFAULT TEXT	DESCRIPTION
		scan		
6	By Devices\ Text Type	Acronis Last backup	(empty)	Date when last successful backup run for the device
7	By Devices\ Text Type	Acronis Last malware scan	(empty)	Date when last successful malware scan run for the device
8	By Devices\ Text Type	Acronis Next backup	(empty)	Date when the next backup run is scheduled for the device
9	By Devices\ Text Type	Acronis Next malware scan	(empty)	Date when the next malware scan run is scheduled for the device
10	By Devices\ Text Type	Acronis Protection plan	(empty)	Protection plan(s) applied to the device. See https://www.acronis.com/en-us/support/documentation/CyberProtectionService/#protection-plans-and-modules.html
11	By Devices\ Text Type	Acronis Status	(empty)	Current protection status for the device: 1. Not protected 2. OK 3. Backup scheduled 4. Running 5. Backing up 6. Scanning 7. Warning 8. Error 9. Critical

Upload scripts

1. Go to **N-able N-central** > **Configuration** > **Scheduled Tasks** > **Script/Software Repository**.
2. Click **Add** and select **Automation policy script type** from the list.
3. In the **Name** field, provide an easily recognizable name, similar to the one of the script's file, then click **OK**.

4. Click **Browse** to locate the script file, downloaded from Acronis.
5. Save the changes.
6. Repeat this procedure for every script.

Note

There is a total of 5 scripts in the .zip file for each OS:

- Acronis Install Agent
- Acronis Uninstall Agent
- Acronis Manage Protection Plan
- Acronis Monitoring
- Acronis Scans

All files with .amp extension represent N-able N-central Automation policies for Windows OS and those with .sh extension - for macOS.

Customer provisioning and deprovisioning

By default, customers are provisioned in **Managed by service provider** mode with the same services enabled as for the service provider and with all quotas set to unlimited.

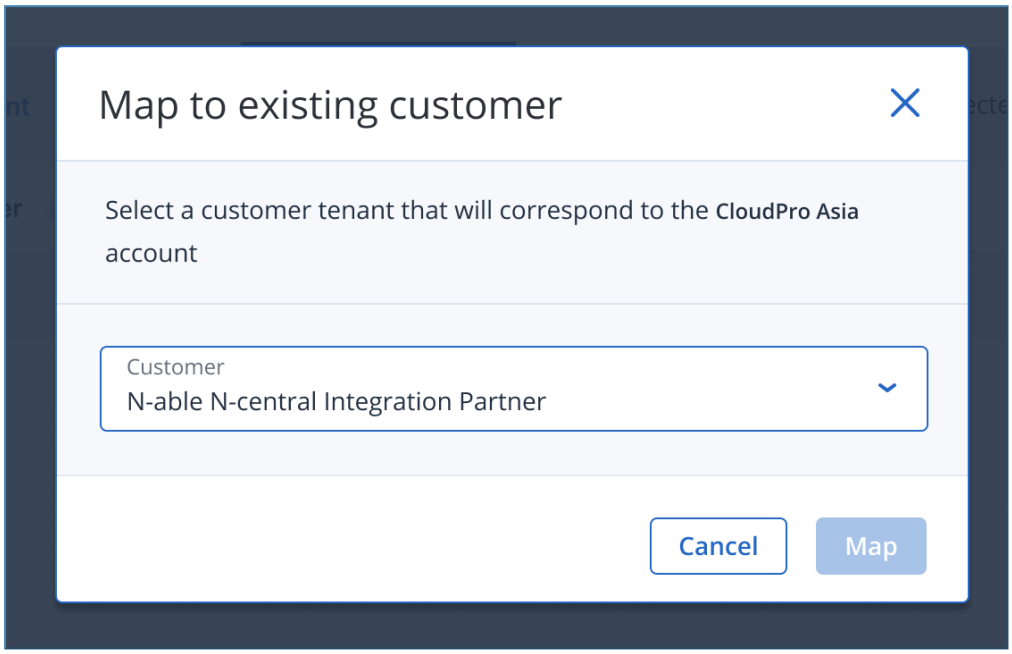
Manual provisioning

RMM customers can be mapped to new or existing customers in Acronis in the following way:

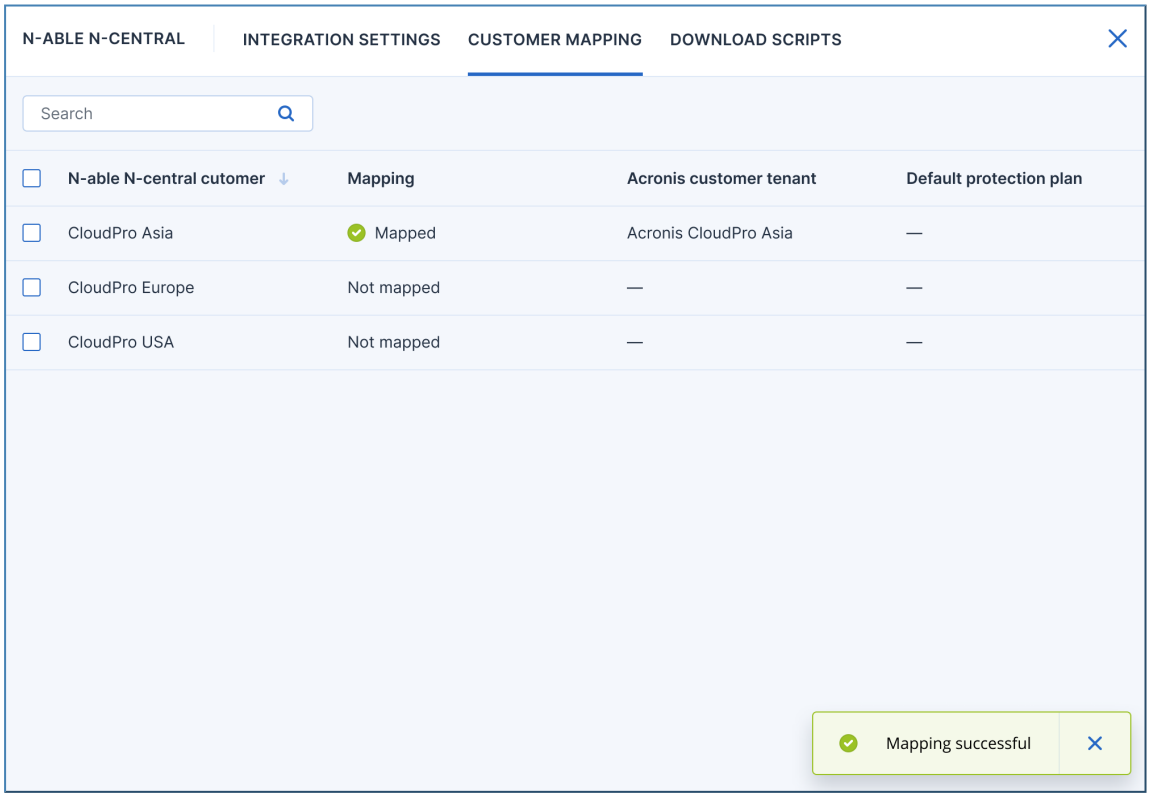
1. Go to **Acronis Management portal** > **Integrations** > **Customer mapping** tab.
2. Make a selection from the **N-able N-Central customer** column (multiple selection is possible when mapping to new customers):

3. Depending on whether you want to map to new or existing customer tenant:
   - Click **Map to new customer tenant**. After a while, the **Mapping** column should display **Mapped** status for this customer.

- Click **Map to existing customer tenant**. A pop-up displays, prompting you to select a customer tenant from the drop-down list, which will correspond to the selected N-able N-central customer account.

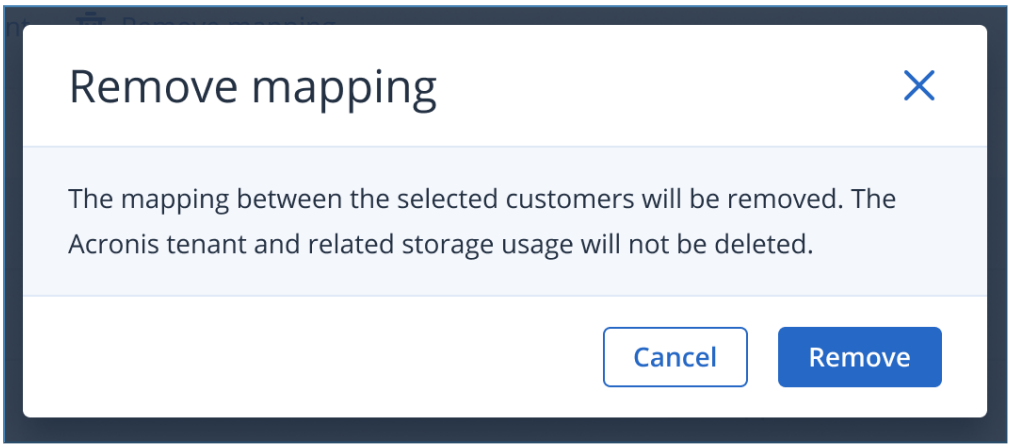


Click **Map**. Then if successful, the **Mapping** column should display the corresponding status.



Remove mapping

To delete the current mapping for a particular selection of customers, use the **Remove mapping** option.
In the pop-up that opens, click **Remove** to confirm:



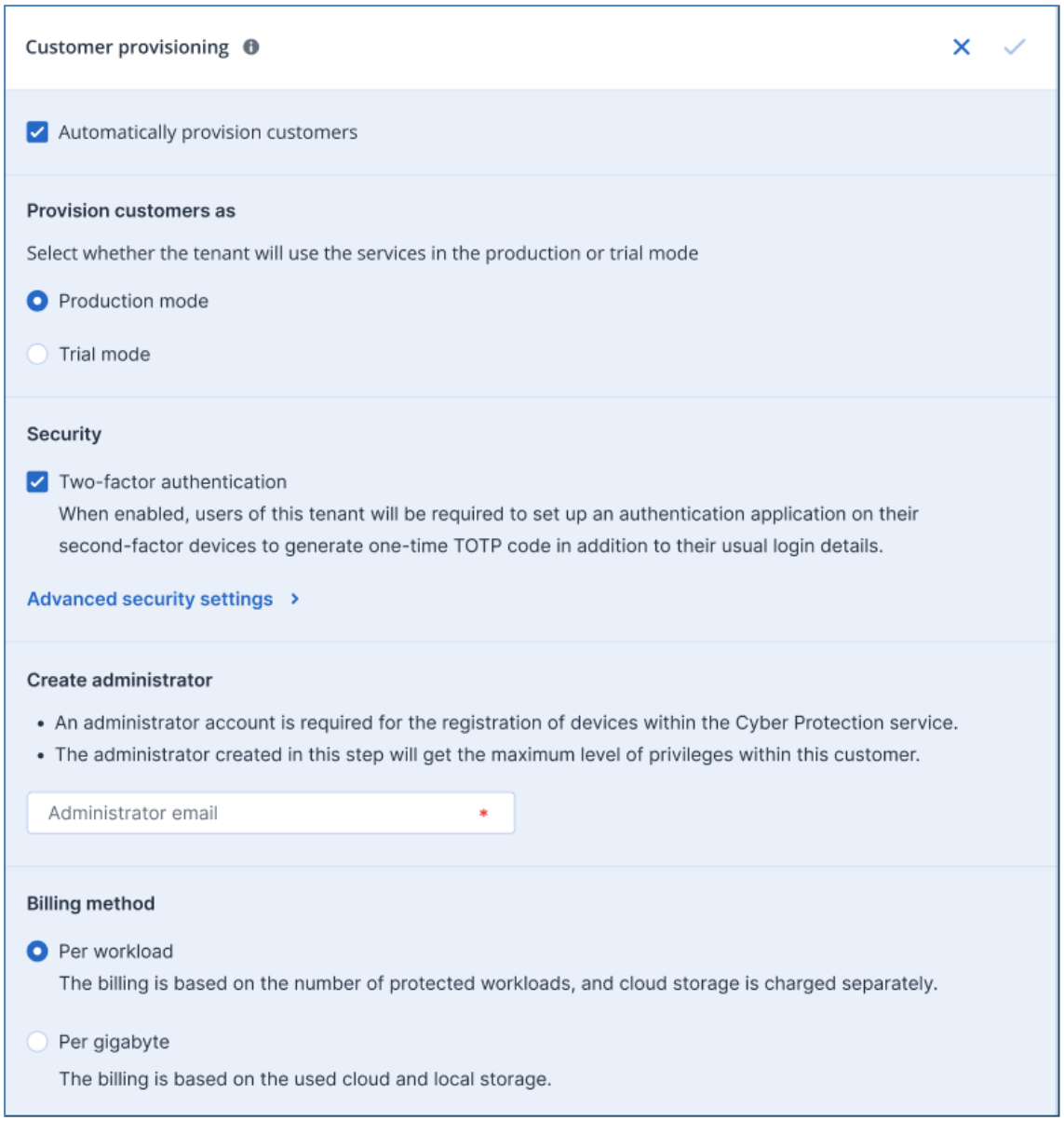
Automatic provisioning

These settings will be used to create customers and accounts in the Management portal.

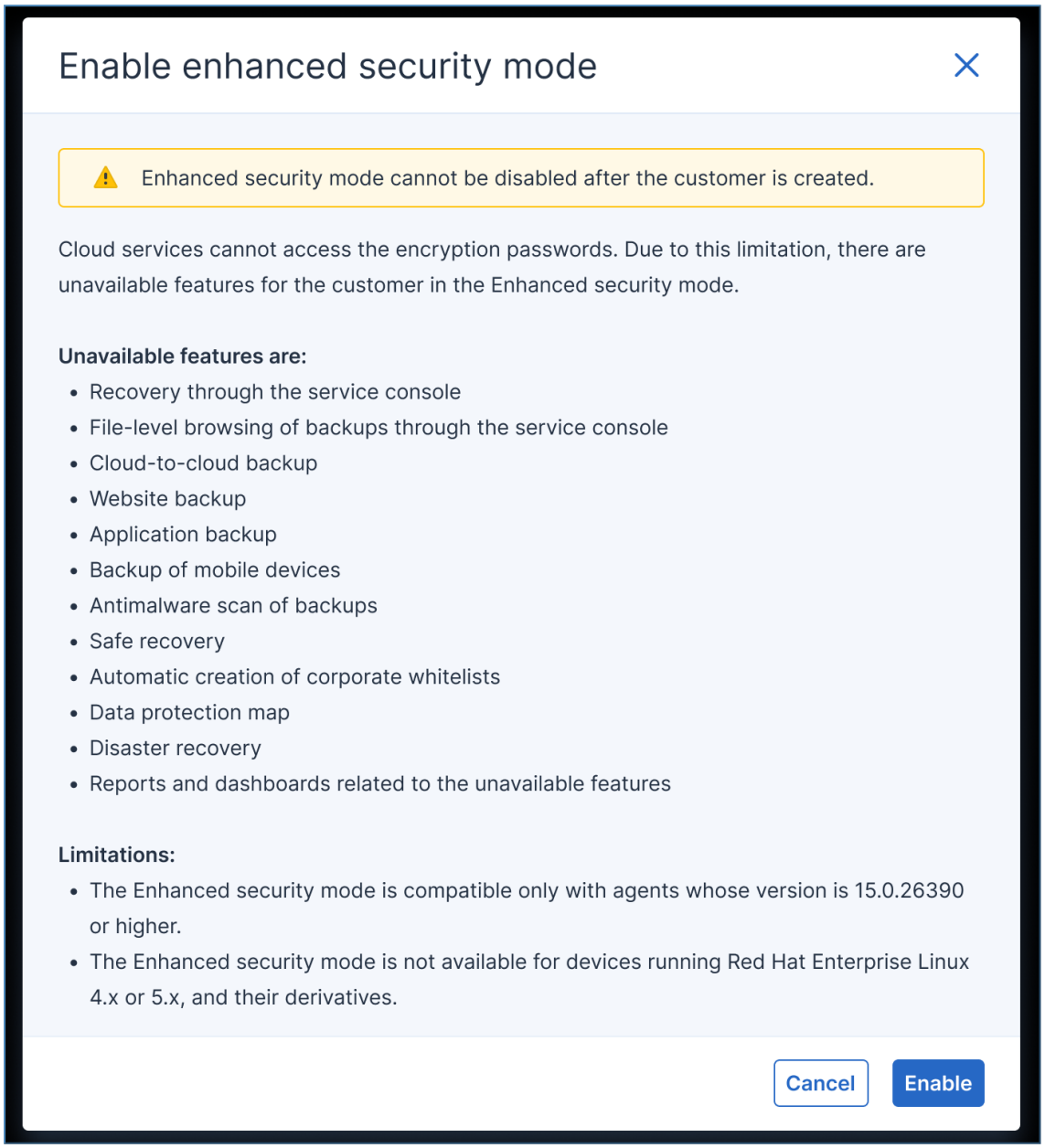
1. Go to **Acronis Management portal** > **Integrations**.
2. Locate the **N-able N-central** tile and click **Configure**.
3. On the **Integration settings** tab, scroll to the **Customer provisioning** section.

4. Click the pencil icon in the top-right corner of this area to open it for editing.
5. The following options should be set:
   a. Select the **Automatically provision customers** checkbox to enable the automatic customers provisioning feature so that new customers appearing in the RMM will be created in Acronis automatically.

b. In the **Provision customers as** field, select either **Trial** or **Production** (default). This is the mode, in which the tenants will use the services.



6. In the **Security** section:
   a. Use the **Two-factor authentication** checkbox to enable or disable 2FA (it is originally turned on) for the admin user that has to be created within the new customer tenant.
   b. Click the **Advanced security settings** link to display the **Enable enhanced security mode** window:

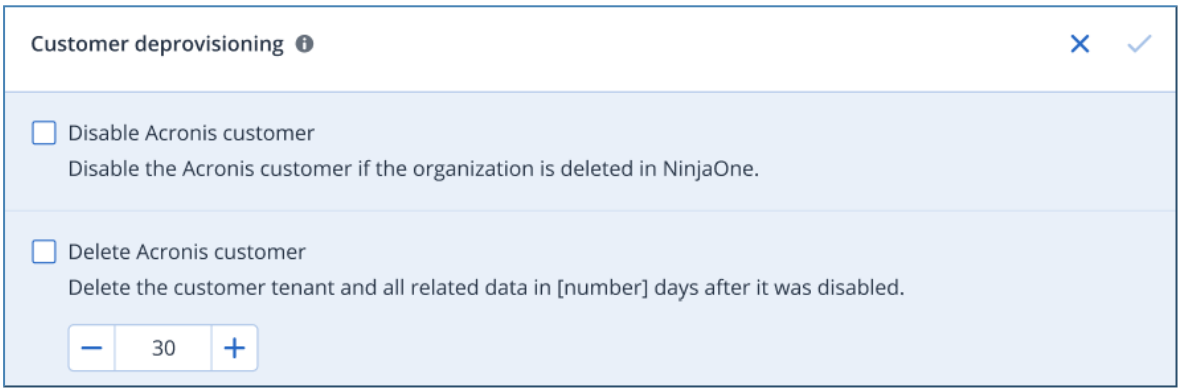


   Review carefully the information available, then click either **Enable** or **Cancel**.
7. In the **Create administrator** field, provide a valid email address of an admin user that has to be created within the new customer tenant. This email will be used to send the activation link.
8. For **Billing method**, select one of the two possible options: **Per workload** (default) or **Per gigabyte**.
9. Click **Save**.

Automatic deprovisioning

These settings will be used to disable and delete customers and accounts in the Management portal.

1. Go to **Acronis Management portal** > **Integrations**.
2. Locate the **N-able N-central** tile and click **Configure**.
3. On the **Integration settings** tab, scroll down to the **Customer deprovisioning** section.
4. Click the pencil icon in the top-right corner of this area to open it for editing.
5. The following options should be set:



- Select the **Disable Acronis customer** checkbox so that already enabled customers will be automatically disabled in Acronis Cyber Protect Cloud after customer deletion in N-able N-central.
- This option can be manipulated only if the previous one has been selected. Then you can mark the **Delete Acronis customer** checkbox to remove customers and all related data in a certain number of days after they were disabled. Provide number of days of your choice or use the **+** and **-** buttons to adjust the value. The default value is 30 days. If you enter 0, customers will be erased immediately after their deletion in N-able N-central.
  To prevent automatic customer deletion, just enable the customer tenant in Acronis before the selected number of days have passed.

6. Click **Save**.

If an automatically disabled customer becomes manually enabled, the integration will leave it as as, without trying to deactivate or remove it again.

Scripts functionality

The following set of macOS scripts are used by the integration of Acronis Cyber Cloud with N-able N-central to deliver various activities:

Script name	Functionality	Necessary arguments
Acronis_ scans	Run one of the following tasks on the current device: • Run a backup • Run malware scan • Run vulnerability assessment	What task to run
Acronis_ monitoring	This script takes all Acronis agent alerts for the device where it runs and inserts them into the AcronisAlerts.log file, located in the same folder where the script is run	None
Acronis_ manage_ protection_ plan	• Apply protection plan • Revoke protection plan	• Registration token • Toggle to set Yes/No
Acronis_ install_agent	• Download installer • Execute installer • Register agent • Optionally, if we have a management token: ◦ Apply protection plan	• Registration token • Data center URL
Acronis_ uninstall_ agent	Uninstall Acronis agent	None

Monitoring

Using custom device properties

1. In N-able N-central, go to **All devices** and select a device.
2. Navigate to **Device Details** and open the **Settings\Custom properties** tab.
3. If the device's customer or site is mapped to an Acronis customer tenant correctly, then in the list you will find Acronis statuses, configured in Define custom properties. These properties will be updated with actual values on a regular basis.

Using Windows Event Log

1. Go to **All devices** in N-able N-central and select a Windows device.
2. Click **Add task** > **Run an Automation policy**.
3. Under **Repository Item**, select **Acronis Monitoring** (or the name of the job defined for the script file upload in "Setting up the integration" (p. 6)).
4. Select target devices.
5. Go to the **Schedule** tab and set a time for N-able N-central to run the task in a recurring manner.
6. Run the script.
7. Click **Views** > **All Devices**.
8. Click the name of the device to set up **Windows Event Log Monitoring**.
9. Navigate to the **Monitoring** tab and click **Add**.
10. Make sure that **Local Agent** is selected in the **Monitoring Appliance** drop-down list.
11. In the **Services** list, set the number of instances of the **Windows Event Log** service to 1 and click **Apply**.
12. Click **Windows Event Log** in the **Service** list.
13. Navigate to the **Service Details** tab to configure the monitoring options.
14. In **Options To Monitor**, select the **Error**, **Information** and **Warning** checkboxes for **Application**.
15. Configure the threshold settings in the **Thresholds** tab according to your personal preferences and click **OK**.
16. The Acronis alerts will be available on the **Reports** tab when filtering by **Application** type of events with **Error**, **Information** and **Warning Event Levels**. Look for Events with **Acronis Agent** Event Source.

Disable the integration

To completely disable the integration, the following is required:

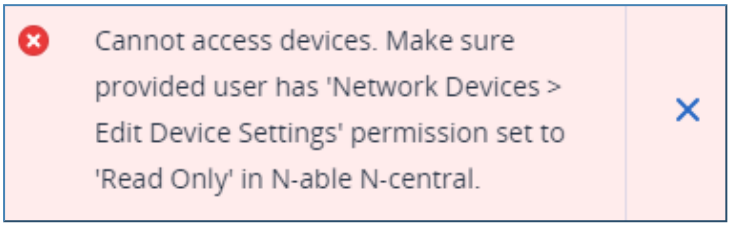
1. In the Acronis Management portal, go to **Integrations**.
2. On the **N-able N-central** integration tile, click on the three dots (**...**) in the top-right and select **Delete** from the drop-down menu.
3. Confirm your selection.

The integration will be disabled and all mapped accounts - disconnected.

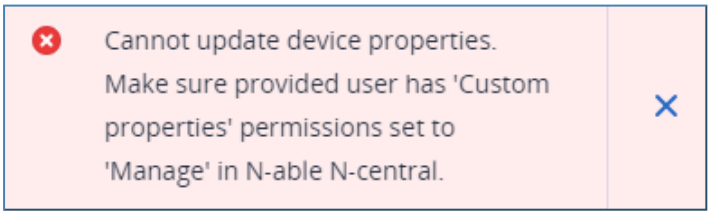
Note
Any Acronis Customer tenants, including their workloads and usages, will not be affected by this action.

Troubleshooting

Here is a list of all possible errors as well as the necessary steps to resolve each of them:

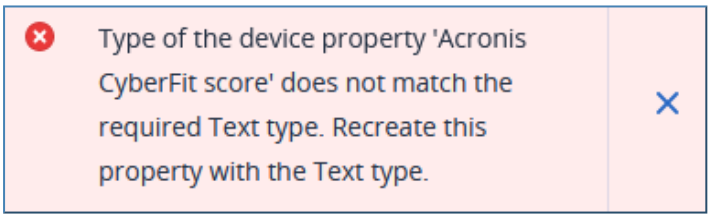


ERROR	CODE	EXPLANATION AND RESOLUTION
"*Cannot access devices. Make sure provided user has "Network Devices > Edit Device Settings" permission set to "Read Only" in N-able N-central.*"	cannotAccessDevices	The API user, configured in the integration (see Configure API user and Enable integration) does not have proper permissions set up in N-able N-central, which disallows the integration to access devices to manage their custom properties. **How to fix:** 1. Go to **Administration** > **User management** > **Roles**. 2. Select the role used for Acronis API user (see Configure API role). 3. Set this role the following permission: "**Network Devices > Edit Device Settings" = "Read Only"**.



ERROR	CODE	EXPLANATION AND RESOLUTION
"*Cannot update device properties. Make sure provided user has "Custom properties" permissions set to "Manage" in N-able N-*	cannotAccessDeviceProperties	The API user, configured in the integration (see Configure API user and Enable integration) does not have proper permissions set up in N-able N-central, which disallows the

ERROR	CODE	EXPLANATION AND RESOLUTION
central."		integration to access devices to update their custom properties. **How to fix:** 1. Go to **Administration** > **User management** > **Roles**. 2. Select the role used for Acronis API user (see Configure API role). 3. Set this role the following permission: **- ADMINISTRATION > CUSTOM PROPERTIES > Create/Edit/Delete = 'Manage' - ADMINISTRATION > CUSTOM PROPERTIES > View/Set = 'Manage'**.



ERROR	CODE	EXPLANATION AND RESOLUTION
"*Type of the device property {label} does not match the required Text type. Recreate this property with the Text type.*"	invalidDeviceProperty	The custom property, mentioned in the error message, does not have the required type (see the list of properties and corresponding types in Define custom parameters). It therefore cannot be updated. **How to fix:** 1. Go to **Administration** > **Custom Properties**. 2. Select the property from the error message. Check if its type corresponds to the required one in Define custom parameters. 3. Delete the property with the wrong type and add a new one.